



FACTA Requirements Drive Changes to Aloha Configurations

The provisions of the U.S. Federal law known as FACTA (Fair and Accurate Credit Transactions Act) contain two requirements that impact the configuration of an Aloha site. One provision requires that a payment card expiration date must not appear in print on receipts, vouchers, or other printed chits in the restaurant. The other requirement specifies that no more than the last five digits of a payment card number may be exposed in print.

Although we recommend suppressing the expiration date and masking all but the last four digits of the payment card in the CISP Compliance Best Practices guide, we felt it would be very helpful to the Aloha POS community to make these changes occur automatically, whenever possible. Beginning with versions of Aloha that become available after November, 2007, the affected settings change automatically to the PCI-compliant state any time you upgrade the Aloha database for a U.S. installation.

The affected settings are as follows:

- In Maintenance > Payments > Tenders > Type tab > Options group box, clear the 'Print Expiration' check box.
- In Maintenance > Store Settings > Credit Card group > Voucher Printing tab, select the 'Suppress Expiration Dates' check box.
- In the same location in Store Settings, immediately beneath the 'Suppress Expiration Dates' option, select 'Only show last 4 digits' from the 'Credit Card Number Mask' drop-down list.

If your installation is outside the U.S., we recommend you verify the legal requirements in your area with regard to printing or suppressing the expiration date and the payment card number. If the regulations under which you operate do not require printing this information, we recommend you configure Aloha to omit printing the expiration date, and to mask all but the last four digits of the payment card number, as a best practice to protect your customers, and your business.

Check with your Radiant Systems representative, to determine if a specific release includes this feature.



EDC Version is Independent of Aloha Version

Credit Card brands are issuing new requirements to meet the increasing security demands of consumers. These changes may require updates to your Aloha EDC software. To quickly react, Radiant Systems is releasing a "version independent" Aloha EDC program. Aloha EDC v6.4 is compatible with Aloha POS v5.3.15 and higher, to eliminate the requirement of full POS upgrades to comply with new card brand or processor requirements.

Important note: Aloha EDC v6.4 requires you to upgrade all security keys to Aloha POS v6.4. When you request new key codes for your lab and/or site(s), specifically request that the key be licensed for v6.4. This upgrade has **NO EFFECT** on your Aloha installation, and does not require an upgrade from your current POS version. For example, you could leave an installation at version 5.3.15 of the POS even though the key would be licensed for v6.4.

Currently Known Upgrade Deadlines

The Product Management team has been working with each credit card processor to understand the required changes and associated deadlines. Upgrade deadlines currently known are as follows:

- Fifth Third clients: February 1, 2008
- First Data Merchant Services (FDMS) clients: April 5, 2008
- CES (FDMS North Platform) clients: April 5, 2008
- Nabanco (FDMS South Platform) clients: April 5, 2008.

We will communicate additional deadlines for implementation as we receive information.

What's New in v6.4?

In addition to POS version independence, EDC v6.4 is currently in controlled deployment and includes the following enhancements:

- Support the following fields for the Bank of America Merchant Services (BAMS) settlement processor:

MasterCard DE22
 Visa ISO 62.23
 AMEX CAPN

Coming Soon...

- Enhance support for American Express pre-paid cards, similar to gift cards. This change will allow pre-paid card authorization based on the card balance and the system will present the balance due for the guest to pay rather than declining the transaction. Note: this will only be support for clients who process direct to AMEX via split dial functionality.
- Support the American Express RFID card called "Express Pay" cards.
- Support high speed authorization and settlement direct to American Express processor.

Clients currently using split dial to process American Express transactions directly to the American Express processor either via dialup or the Merchant Link gateway will be required to migrate to the CAPN solution prior to July 1, 2008. While merchants will NOT be required to change their SE number, they WILL need to be set up with a new Submitter ID if they wish to continue processing directly to American Express. The other logistics of this migration are currently being discussed with American Express and will be communicated in future announcements.

Please email prodmgmt@radiantsystems.com with any questions.

Disabling Alt+X Access to Aloha Mandatory for PCI DSS Compliance!

In the last edition of the Compliance newsletter, we announced that the Alt+X method of accessing Aloha QuickService, TableService, and EDC is no longer available, beginning with Aloha POS v6.3.

We also mentioned that you can disable this method of access for all prior versions of these products. To comply with PCI DSS requirements for versions of Aloha older than v6.3, you must disable the Alt+X login method of access – **it is mandatory for compliance!** Before disabling this feature in live sites, be sure to configure appropriate back office security levels and users with strong passwords, as outlined in the CISP Best Practices Guide. Refer to RKS ID 6298 for the procedure to disable Alt+X access to the Aloha system for all versions prior to v6.3. Please contact your Radiant Systems representative if you cannot access the Radiant Knowledge System (RKS) to obtain this document.





Good News for Aloha Enterprise.com Customers!

We have good news for customers of Aloha Enterprise.com! Beginning with v9.1, when data is imported from the Aloha system to Enterprise.com, the process automatically masks payment card numbers, regardless of the configuration in the Aloha system. The exceptions to automatic card number masking are eCards and house account cards. Customer intervention is unnecessary, as this new process is the default configuration.

In addition to masking card numbers during data imports, Aloha Enterprise.com has also already masked card numbers in all legacy data. Currently, any historical customer data stored at Level 3 contains no unmasked payment card numbers.



What's New in PCI?

The Payment Card Industry Security Standards Council (PCI) has initiated several changes in the Data Security Standard (DSS) requirements in the version currently available from them. You can obtain a copy of the current standards from the following Internet address:

https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

The impact of these new requirements on sites using Aloha varies from the direct to the oblique, as summarized in the following table:

Change to PCI Security Standard	Impact on site using Aloha
<p>Hosting providers must protect the data and hosted environment of each entity by adhering to the PCI DSS.</p> <p>Refer to Sections 2.4 and Appendix A in the PCI DSS document for the requirements to which hosting providers must conform to protect cardholder data and to keep separate the data of each connected entity</p>	<p>Effective with the v9.1 release of Enterprise.com, payment card data will be masked upon import, regardless of the configuration in the Aloha system. In addition, historical customer data stored at Level 3 contains no unmasked payment card numbers.</p>
<p>Antivirus software used in payment card sites must now also detect, remove, and protect against other forms of malicious software, including spyware and adware.</p> <p>Refer to Section 5.1.1 in the PCI DSS document.</p>	<p>Sites must upgrade their antivirus software to more capable versions, or change to more capable products.</p>
<p>Application security specialists must review Web-facing applications for vulnerabilities, or install an application layer firewall in front of all Web-facing applications.</p> <p>Note: This is a 'best practice' until it becomes a requirement, 6/30/08.</p> <p>Refer to Section 6.6 in the PCI DSS document.</p>	<p>Security specialists must review Web-facing Radiant products and services for vulnerabilities, or sites must install and maintain an application layer firewall in front of all Web-facing applications hosted by Radiant.</p>
<p>Processors and service providers must maintain and implement policies and procedures to manage connected entities in a secure manner.</p> <p>Refer to Section 12.10 in the PCI DSS document.</p>	<p>Processors and service providers are required to implement and maintain policies and procedures that ensure proper due diligence is conducted prior to connecting to a merchant, and to verify the connecting merchant is PCI DSS compliant. Processors and service providers must also follow established processes to connect and disconnect merchants.</p>
<p>Entities that cannot conform to the PCI DSS requirements must use compensating controls to secure cardholder data.</p> <p>Refer to the new Appendix B in the PCI DSS document for a discussion on compensating controls.</p>	<p>If a site is unable to conform to PCI DSS requirements, the site must use compensating controls for securing cardholder data.</p>



PCI and State Legislative Initiatives

You have often heard phrases like ‘...it ought to be a law...’ in conversation. Well, soon ‘it’ may be a law in your neighborhood. The PCI Data Security Standards (PCI DSS), or parts of it, are becoming the basis for legislative initiatives in various states, such as Minnesota, Texas, Massachusetts, California, and New Jersey.

The U.S. House of Representatives also has legislation going together that would hold merchants responsible for expenses financial institutions incur as a result of security breaches. All of these initiatives appear to be independent of, and in addition to, the penalties already in place.

These forces, arrayed to make merchants and payment card applications PCI DSS compliant, serve to point up the importance of our joint efforts to make sure every Aloha installation, regardless of the level of business, complies with these security standards. We recommend you obtain the CISP Compliance Best Practices guide that applies to the version of Aloha you are using, and use it as a starting point for configuring your sites for maximum security. We also recommend you take advantage of the ever improving security features by upgrading to the latest version of Aloha available.

If you have any questions, please contact your Radiant Systems representative for help getting the answers you need.